BITAG
Broadband Internet Technical Advisory Group

1550 Larimer Street, Suite 168
Denver, CO. 80202

Contact: info@bitag.org

BITAG Publishes Report:
Internet of Things (IoT) Security and Privacy Recommendations

Report explores the technical aspects of the security and privacy of networked consumer devices

Denver, CO (November 22, 2016): Today, the Broadband Internet Technical Advisory Group (BITAG) announced the publication of its report on the technical aspects of Internet of Things (IoT) security and privacy. The executive summary of the report is attached here, and the report itself can be found at: http://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php

In the past few years, many devices now being connected to the Internet are not only personal computers but also a variety of devices embedded with Internet connectivity and functions. This class of devices has generally been described as the *Internet of Things* (IoT) and has brought with it new security and privacy risks.

Although consumers face general security and privacy threats as a result of *any* Internet-connected device, the nature of consumer IoT is unique because it can involve non-technical or uninterested consumers; challenging device discovery and inventory on consumer home networks as the number and variety of devices proliferate; negative effects on the Internet access service of both the consumer and others that run on shared network links; and effects on other Internet services when these devices are compromised by malware and become a platform for unwanted data traffic—such as spam and denial of service attacks—which can interfere with the provision of these other services. Importantly, the number and diversity of consumer IoT devices is growing rapidly, and these devices often function autonomously, without human intervention.

Several recent incidents have demonstrated that some devices do not abide by rudimentary privacy and security best practices. In some cases, devices have been compromised and allowed unauthorized users to perform Distributed Denial of Service (DDoS) attacks, perform surveillance and monitoring, gain unauthorized access or control, induce device or system failures, and disturb or harass authorized users or device owners.

Potential issues contributing to the lack of privacy and security best practices include: lack of IoT supply chain experience with security and privacy, lack of incentives to develop and deploy updates after the initial sale, lack of secure over-the-network software updates, devices with malware inserted during the manufacturing process, and more.

The emergence of IoT presents opportunities for significant innovation, from smart homes to smart cities. In many cases, straightforward changes to device development, distribution, and maintenance processes can prevent the distribution of IoT devices that suffer from significant security and privacy issues. BITAG believes the recommendations outlined in this report may help to dramatically improve the security and privacy of IoT devices and minimize the costs associated with collateral damage. In addition, unless the IoT device sector—the sector of the industry that manufactures and distributes these devices—improves device security and privacy, consumer backlash may impede the growth of the IoT marketplace and ultimately limit the promise that IoT holds.

The lead editors of BITAG's report on the Internet of Things (IoT) Security and Privacy Recommendations were Jason Livingood, Vice President - Technology Policy & Standards at Comcast and Nick Feamster, Professor of Computer Science at Princeton University. Douglas Sicker, Executive Director of BITAG, Chair of BITAG's Technical Working Group, Department Head of Engineering and Public Policy and a professor of Computer Science at Carnegie Mellon University, chaired the review itself.

About BITAG. BITAG is a non-profit, multi-stakeholder organization focused on bringing together engineers and technologists in a Technical Working Group (TWG) to develop consensus on broadband network management practices and other related technical issues that can affect users' Internet experience, including the impact to and from applications, content and devices that utilize the Internet.

This is BITAG's ninth technical report. BITAG's recent reports have focused on: differentiation of Internet traffic, Internet interconnection, real-time network management of Internet congestion, and port blocking, among other topics. Copies of these technical reports can be found on the BITAG website at www.bitag.org.

Questions, Suggestions or Topics? BITAG welcomes any questions, comments or suggestions. Also, if you are interested in submitting a technical review request to BITAG, please contact our Deputy Director, Kaleb Sieh, at ksieh@bitag.org.

– ATTACHMENT –

Executive Summary: Internet of Things (IoT) Security and Privacy Recommendations

Full report: http://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php

In the past few years, many of the new devices connected to the Internet have not been personal computers, but rather a variety of devices embedded with Internet connectivity and functions. This class of devices has generally been described as the *Internet of Things* (IoT) and has brought with it new security and privacy risks.

The term "IoT" has potentially broad scope. IoT can refer to deployments in homes, businesses, manufacturing facilities, transportation industries, and elsewhere. Thus, IoT can refer to much more than simply consumer-oriented devices. For the purposes of this report, the term IoT is used to refer solely to consumer-oriented devices and their associated local and remote software systems, though some or all of the recommendations may be more broadly applicable. This report is concerned with scenarios where consumers are installing, configuring, and administering devices that they lease or own.

The number and diversity of consumer IoT devices is growing rapidly; these devices offer many new applications for end users, and in the future will likely offer even more. Many IoT devices are either already available or are being developed for deployment in the near future, including:

- sensors to better understand patterns of daily life and monitor health
- monitors and controls for home functions, from locks to heating and water systems
- devices and appliances that anticipate a consumer's needs and can take action to address them (e.g., devices that monitor inventory and automatically re-order products for a consumer)

These devices typically interact with software running elsewhere on the network and often function autonomously, without requiring human intervention. In addition, when coupled with data analysis and machine learning, IoT devices may be able to take more proactive actions, reveal interesting and useful data patterns, or make suggestions to end users that may improve their health, environment, finances, and other aspects of their lives.

Although consumers face general security and privacy threats as a result of *any* Internet-connected device, the nature of consumer IoT is unique in that it can involve non-technical or uninterested consumers, challenging device discovery and inventory on consumer home networks as the number and variety of devices proliferate, impacts on the Internet access service of both the consumer and others that run on shared network links, and effects on other services in that when IoT devices are compromised by malware they can become a platform for unwanted data traffic—such as spam and denial of service attacks—which can interfere with the provision of these other services.

Several recent reports have shown that some devices do not abide by rudimentary security and privacy best practices. In some cases, devices have been compromised and allowed unauthorized users to perform surveillance and monitoring, gain access or control, induce device or system failures, and disturb or harass authorized users or device owners.

Potential issues contributing to the lack of security and privacy best practices include: lack of IoT supply chain experience with security and privacy, lack of incentives to develop and deploy updates after the initial sale, difficulty of secure over-the-network software updates, devices with constrained or limited hardware resources (precluding certain basic or "common-sense" security measures), devices with constrained or limited user-interfaces (which if present, may have only minimal functionality), and devices with malware inserted during the manufacturing process.

The emergence of IoT presents opportunities for significant innovation, from smart homes to smart cities. In many cases, straightforward changes to device development, distribution, and maintenance processes can prevent the distribution of IoT devices that suffer from significant security and privacy issues. BITAG believes that following the guidelines outlined in this report may dramatically improve the security and privacy of IoT devices and minimize the costs associated with the collateral damage that would otherwise affect both end users and ISPs. In addition, unless the IoT device sector—the sector of the industry that manufactures and distributes these devices—improves device security and privacy, consumer backlash may impede the growth of the IoT marketplace and ultimately limit the promise IoT holds.

Observations. From the analysis made in this report and the combined experience of its members when it comes to Internet of Things devices, the BITAG Technical Working Group makes the following *observations*:

- **Security Vulnerabilities:** Some IoT devices ship "from the factory" with software that either is outdated or becomes outdated over time. Other IoT devices may ship with more current software, but vulnerabilities may be discovered in the future. Vulnerabilities that are discovered throughout a device's lifespan may make a device less secure over time unless it has a mechanism to subsequently update its software.

- **Insecure Communications:** Many of the security functions designed for more general-purpose computing devices are difficult to implement on IoT devices and a number of security flaws have been identified in the field, including unencrypted communications and data leaks from IoT devices.
    - **Unauthenticated Communications:** Some IoT devices provide automatic software updates. Without authentication and encryption, however, this approach is insufficient because the update mechanism could be compromised or disabled. In addition, many IoT devices do not use authentication in the course of communicating.
    - **Unencrypted Communications:** Many IoT devices send some or all data in cleartext, rather than in an encrypted form. Communications in cleartext can be observed by other devices or by an attacker.
    - **Lack of Mutual Authentication and Authorization:** A device that allows an unknown or unauthorized party to change its code or configuration, or to access its data, is a threat. The device can reveal that its owner is present or absent, facilitate the installation or operation of malware, or cause its core IoT function to be fundamentally compromised.
    - **Lack of Network Isolation:** These devices also create new risks and are susceptible to attacks *inside* the home. Because many home networks do not, by default, isolate different parts of the network from each other, a network-connected device may be able to observe or exchange traffic with other devices on the same home network, thus making it possible for one device to observe or affect the behavior of unrelated devices.

- **Data Leaks:** IoT devices may leak private user data, both from the cloud (where data is stored) and between IoT devices themselves.
  - **Leaks from the Cloud:** Cloud services could experience a data breach due to an external attack or an insider threat. Additionally, if users rely on weak authentication or encryption methods for these cloud-hosted services, user data may also be compromised.
  - **Leaks from and between Devices:** In some cases, devices on the same network or on neighboring networks may be able to observe data from other devices such as the names of people in a home, the precise geographic location of a home, or even the products that a consumer purchases.

- **Susceptibility to Malware Infection and Other Abuse:** Malware and other forms of abuse can disrupt IoT device operations, gain unauthorized access, or launch attacks.

- **Potential for Service Disruption:** The potential loss of availability or connectivity not only diminishes the functionality of IoT devices, but also may degrade the security of devices in some cases such as when an IoT device can no longer function without such connectivity (e.g., a home alarm system deactivating if connectivity is lost).

- **Potential That Device Security and Privacy Problems Will Persist:** IoT device security issues are likely to persist because many devices may never receive a software update, either because the manufacturer (or other party in the IoT supply chain, or IoT service provider) may not provide updates or because consumers may not apply the updates that are already available.
  - **Many IoT Devices Will Never Be Fixed:** Deploying software updates that patch critical security vulnerabilities is difficult in general. Many device vendors and manufacturers do not have systems or processes to deploy software updates to thousands of devices, and deploying over-the-network updates to devices that are operating in consumer homes is difficult, as updates can sometimes interrupt service and sometimes have the potential to "brick" the device, if done improperly. Additionally, some devices may not even be capable of software updates.
  - **Software Updates Address More Than Just Bugs:** Software updates are not simply intended to fix security or privacy bugs. They may also be intended to introduce major new functions, or improve performance and security.
  - **Consumers Are Unlikely to Update IoT Device Software:** Few end users consistently update device software of their own accord; it is best to assume that most end users will never take action on their own to update software.

- **Device Replacement May be an Alternative to Software Updates – for Inexpensive or "Disposable" Devices:** In some cases, replacing a device entirely may be an alternative to software updates. Certain IoT devices may be so inexpensive that updating software may be impractical or not cost-effective.

Recommendations. The BITAG Technical Working Group also has the following *recommendations*:

- **IoT Devices Should Use Best Current Software Practices:**
  - **IoT Devices Should Ship with Reasonably Current Software:** BITAG recommends that IoT devices should ship to customers or retail outlets with reasonably current software that does not contain severe, known vulnerabilities.
  - **IoT Devices Should Have a Mechanism for Automated, Secure Software Updates:** Software bugs should be minimized, but they are inevitable. Thus, it is critical for an IoT device to have a mechanism for automatic, secure software updates. BITAG recommends that manufacturers of IoT devices or IoT service providers should therefore design their devices and systems based on the assumption that new bugs and vulnerabilities will be discovered over time. They should design systems and processes to ensure the automatic update of IoT device software, without requiring or expecting any type of user action or even user opt-in.
  - **IoT Devices Should Use Strong Authentication by Default:** BITAG recommends that IoT devices be secured by default (e.g. password protected) and not use common or easily guessable user names and passwords (e.g., "admin", "password").
  - **IoT Device Configurations Should Be Tested and Hardened:** Some IoT devices allow a user to customize the behavior of the device. BITAG recommends that manufacturers test the security of each device with a range of possible configurations, as opposed to simply the default configuration.

- **IoT Devices Should Follow Security & Cryptography Best Practices:** BITAG recommends that IoT device manufacturers secure communications using Transport Layer Security (TLS) or Lightweight Cryptography (LWC). If devices rely on a public key infrastructure (PKI), then an authorized entity must be able to revoke certificates when they become compromised, and manufacturers should take care to avoid encryption methods, protocols, and key sizes with known weaknesses. Additional encryption best practices include:
  - Encrypt Configuration (Command & Control) Communications By Default
  - Secure Communications To and From IoT Controllers
  - Encrypt Local Storage of Sensitive Data
  - Authenticate Communications, Software Changes, and Requests for Data
  - Use Unique Credentials for Each Device
  - Use Credentials That Can Be Updated
  - Close Unnecessary Ports and Disable Unnecessary Services
  - Use Libraries That Are Actively Maintained and Supported

- **IoT Devices Should Be Restrictive Rather Than Permissive in Communicating:** When possible, devices should not be reachable via inbound connections by default. IoT devices should not rely on the network firewall alone to restrict communication, as some communication between devices within the home may not traverse the firewall.

- **IoT Devices Should Continue to Function if Internet Connectivity is Disrupted:** BITAG recommends that an IoT device should be able to perform its primary function or functions (e.g., a light switch or a thermostat should continue to function with manual controls), even if it is not connected to the Internet because Internet connectivity may be disrupted due to causes ranging from accidental misconfiguration to intentional attack. IoT devices that have implications for user safety should continue to function under disconnected operation to protect the safety of consumers.

- **IoT Devices Should Continue to Function If the Cloud Back-End Fails:** Many services that depend on or use a cloud back-end can continue to function, even if in a degraded or partially functional state, when connectivity to the cloud back-end is interrupted or the service itself fails.

- **IoT Devices Should Support Addressing and Naming Best Practices:** Many IoT devices may remain deployed for a number of years after they are installed. Supporting the latest protocols for addressing and naming will ensure that these devices remain functional for years to come.
    - **IPv6:** BITAG recommends that IoT devices support the most recent version of the Internet Protocol, IPv6.
    - **DNSSEC:** BITAG recommends that IoT devices support the use or validation of DNS Security Extensions (DNSSEC) when domain names are used.

- **IoT Devices Should Ship with a Privacy Policy That is Easy to Find & Understand:** BITAG recommends that IoT devices ship with a privacy policy, but that policy must be easy for a typical user to find and understand.

- **Disclose Rights to Remotely Decrease IoT Device Functionality:** BITAG recommends that if the functionality of an IoT device can be remotely decreased by a third party, such as by the manufacturer or IoT service provider, this possibility should be made clear to the user at the time of purchase.

- **The IoT Device Industry Should Consider an Industry Cybersecurity Program:** BITAG recommends that the IoT device industry or a related consumer electronics group consider the creation of an industry-backed program under which some kind of "Secure IoT Device" logo or notation could be carried on IoT retail packaging. An industry-backed set of best practices seems to be the most pragmatic means of balancing innovation in IoT against the security challenges associated with the fluid nature of cybersecurity, and avoiding the "checklist mentality" that can occur with certification processes.

- **The IoT Supply Chain Should Play Their Part In Addressing IoT Security and Privacy Issues:** End users of IoT devices depend upon the IoT supply chain, from manufacturer to retailer, to protect their security and privacy, and some or all parts of that IoT supply chain play a critical role throughout the entire lifecycle of the product. In addition to other recommendations in this section, BITAG recommends that the IoT supply chain takes the following steps:
    - **Privacy Policy:** Devices should have a privacy policy that is clear and understandable, particularly where a device is sold in conjunction with an ongoing service.

- **Reset Mechanism:** Devices should have a reset mechanism for IoT devices that clears all configuration for use when a consumer returns or resells the device. The device manufacturers should also provide a mechanism to delete or reset any data that the respective device stores in the cloud.
- **Bug Reporting System:** Manufacturers should provide a bug reporting system with a well-defined bug submission mechanisms and documented response policy.
- **Secure Software Supply Chain:** Manufacturers should protect the secure software supply chain to prevent introduction of malware during the manufacturing process; vendors and manufacturers should take appropriate measures to secure their software supply chain.
- **Support IoT Device for Entire Lifespan:** Manufacturers should support an IoT device throughout the course of its lifespan, from design to the time when a device is retired, including transparency about the timespan over which they plan to provide continued support for a device, and what the consumer should expect from the device's function at the end of the device's lifespan.
- **Clear Contact Methods:** Manufacturers should provide clear methods for consumers to determine who they can contact for support and methods to contact consumers to disseminate information about software vulnerabilities or other issues.
- **Report Discovery and Remediation of Vulnerabilities:** Manufacturers should report discovery and remediation of software vulnerabilities that pose security or privacy threats to consumers.
- **Clear Vulnerability Reporting Process:** Manufacturers should provide a vulnerability reporting process with a well-defined, easy-to-locate, and secure vulnerability reporting form, as well as a documented response policy.